GOVERNMENT COMMUNICATIONS SECURITY BUREAU

UPDATED PRIVACY IMPACT ASSESSMENT: ENHANCING CYBER SECURITY PROJECT

[Name removed under section 6(a) of the Official Information Act 1982]

March 2015

THIS PAGE INTENTIONALLY LEFT BLANK

OVERVIEW

i. The Government Communications Security Bureau proposes to undertake a programme of discrete cyber security related activities collectively known as CORTEX. To that end it has sought Privacy Impact Assessments. This is the second such assessment.

ii. The first assessment was provided in April 2014 then supplemented in May 2014 by the addition of an Executive Summary. That assessment needs to be updated for the following reasons.

   a. Certain aspects of the proposed activities have changed.

   b. The first assessment made recommendations to mitigate the privacy impacts of Project activity. GCSB has acted upon certain of those recommendations.

iii. This updated assessment takes these changes into account. Some changes are also made to more clearly present the underlying analysis, including by adopting terminology that has since been adopted by GCSB personnel.

EXECUTIVE SUMMMARY

This PIA considers more than GCSB's legal obligations

i. Each of the activities that the Government Communications Security Bureau proposes to undertake as part of Project CORTEX entails the screening of internet communications of certain entities for the purpose of detecting cyber threats. Because such communications include "personal information", CORTEX activities are regulated by the Privacy Act and other privacy-related requirements.

ii. Not all of the twelve "Privacy Principles" set out in the Privacy Act apply to GCSB. However, this Privacy Impact Assessment assesses privacy impacts by reference to all twelve. In this respect, this assessment accords with best-practice advice of the Office of the Privacy Commissioner.

CORTEX activity does not strongly implicate certain privacy interests

iii. The privacy impacts of CORTEX activities are significantly mitigated by context – most particularly by the fact that information is not collected for the purpose of harvesting its "content" in the sense contemplated by the Privacy Act. Unlike collection activities of, say, retailers (seeking to profile their customer base) or Government agencies (requiring information to support the administration of Government services), communications are not collected under CORTEX to develop an understanding of the communicants. The purpose of collection is simply the detection and, in some cases, disruption of cyber attacks. Communications are intercepted only because they constitute a potential vector for such attacks.

iv. The fact that "collected" information is not used for its informational content renders certain of the "Privacy Principles" set forth in the Privacy Act (certain of which are reflected in requirements of the GCSB Act) far less relevant than otherwise.

v. For example, the principle requiring agencies that collect information to ensure that collected information is "accurate, up to date, complete, relevant, and not misleading" is inapposite where information is collected not for the "accuracy" of what it might say about the communicant but simply because it might contain malware. In this sense, even internet traffic

comprising solely computer-to-computer communications (for the purpose of facilitating human-to-human communications) is collected in support of CORTEX activities.

vi. Because the Privacy Principles are interdependent, this observation has cascading effects. For example, certain privacy principles require affected persons to be notified of the fact of collection, advised of their rights to seek access to collected information and given opportunity to seek the "correction" of collected information. Others require that information about individuals be collected from those individuals. To the extent that these principles protect the privacy interests in "informational accuracy", they too are less relevant than otherwise.

vii. Privacy impacts are also significantly mitigated by the fact that CORTEX activities are information assurance activities of a kind commonly (sometimes ubiquitously) undertaken by organisations for the purpose of protecting their computer systems from malware. Affected persons are, therefore, less likely to hold expectations that internet traffic will not be collected for that purpose – and even less likely to hold "reasonable" expectations in this respect.

Controls over storage, use and destruction are key – and these are extraordinary

viii. Regardless of the purpose of collection, "personal information", once collected, must be used only for proper purposes and protected from improper use. The Privacy Principles regulating storage, use and destruction of information are key principles in the context of CORTEX activity.

ix. Being an intelligence agency, GCSB has extraordinary "information security" (INFOSEC) controls. These range from cultural norms, supported by rigorous security vetting requirements and physical INFOSEC controls, to complex technical capabilities enabling controlled access to quarantined information.

There is strong, independent institutional oversight of these controls

x. CORTEX activities are currently undertaken pursuant to a warrant or authorisation issued by the Minister Responsible for the GCSB and the Commissioner of Security Warrants. This is not projected to change (although Capability 5 does not qualify as warrantable activity, that activity entails only the use, not the collection of, information that is collected pursuant to warrant).

xi. Under the GCSB Act, such warrants/authorisations may be issued only if the Minister and Commissioner are satisfied of the need for collection and only if there are "satisfactory arrangements" regulating the extent and manner of collection and the handling of collected information. The warranting process focuses closely upon protections against potential misuse of information.

xii. This process is supported by the obligations of the Inspector-General of Intelligence and Security to audit the internal policies and processes of GCSB, including policies and practices relied upon to justify the issuing of warrants and authorisations.

xiii. This framework is clearly intended to safeguard the privacy interests of affected persons.

Where Privacy Principles are not adhered to, "non-compliance" is permitted

xiv. Not all of the Privacy Principles can be adhered to in undertaking the proposed CORTEX activities. Significantly, those that cannot are either principles with which GCSB is not required to comply (given the exemptions that apply to intelligence agencies under the Privacy Act) or principles that are expressly subject to applicable exemptions.

xv. For example, contrary to Privacy Principle 3, GCSB will not notify affected persons of the fact that GCSB will be screening their communications for information assurance purposes. The privacy impacts of this are significantly mitigated by the likelihood that affected persons would reasonably expect (or be expressly advised) that their communications would (somehow) be collected for this purpose. Also, Principle 3 is not a principle with which GCSB must comply. Even if it did apply, failure to notify would be justified by reference to an applicable exemption, namely the exemption that applies where notification would prejudice the purpose of collection.

Recommendations

xvi. The standard term contained in written agreements with entities receiving services under CORTEX is broad enough to oblige them to notify not only internal but also external users of their systems that communications will be collected for information assurance purposes. However, it does not expressly identify external users and could be construed as limited to only internal users. Further, the means through which GCSB expects this requirement to be met are not means that necessarily entail notification to external users. Although GCSB personnel have advised that this standard term is nonetheless construed by the recipient entities as obliging ANI to take these measures, it is recommended that it expressly require entities to notify external users that communications via affected systems will be accessed for information assurance purposes.

xvii. Because of the nature of CORTEX activity, the extraordinary INFOSEC controls that GCSB is able to implement and the strong, independent oversight over their implementation, the potential privacy impacts of CORTEX activity are by and large appropriately mitigated. Some recommendations are suggested. In particular, it is recommended that:

a. GCSB develop a retention and destruction policy for each Project activity, taking into account (i) the differing benefits of retention in each case and (ii) the potential need for even data qualifying for extended retention to be destroyed at some stage; and

b. to minimise the potential for a breach of sharing restrictions, GCSB should seek consistency in how these restrictions are expressed in warrants/authorisations and in written agreements with recipient entities.

1. INTRODUCTION

Background

1. The Government Communications Security Bureau requires a Privacy Impact Assessment (PIA) relating to certain activities comprising the "Enhancing Cyber Security Project" (the Project).
2. The Project comprises a programme of discrete activities collectively known as CORTEX.
3. These activities share a common purpose of enhancing New Zealand's cyber security through the provision of information assurance and cyber security (IACS).
4. The provision of IACS is a core GCSB function under s 8A of its governing act, the Government Communications Security Bureau Act 2003. The Project is key to the performance of that function. It has four key objectives, as set out below.

Objective	Summary
Information systems are less vulnerable to advanced malware	Deny
Widen detection of known advanced malware	Detect
Increase discovery of unknown advanced malware	Discover
Advanced malware is actively disrupted through technical means	Disrupt

5. The focus of the Project is upon the provision of enhanced cyber security services to selected "assets of national interest" (ANI), such as subsets of public agencies, critical national infrastructure and key economic generators.

Purpose

6. The main deliverable is a report that:
   a) evaluates the potential for privacy impacts in terms of likelihood, scale and nature; and
   b) identifies mitigating measures that might be required to render Project activities:
   c) lawful; and
   d) appropriate.

Initial comments

Section 25A is not the only relevant consideration

7. As the following analysis explains, s 25A of the GCSB Act requires the preparation of an information privacy policy. The purpose of such a policy is to give effect to certain specified "principles" in a manner that is "compatible with the requirements of national security". Certain of these principles map to "information privacy principles" contained in the Privacy Act 1993.
8. These s 25A principles are not the only factors relevant to any GCSB "privacy compliance" assessment. Certain (though not many) of the information privacy principles apply to GCSB under the Privacy Act itself. Further, the privacy framework within which GCSB must operate is significantly affected by other provisions of the GCSB Act that serve to control GCSB activity – most particularly the interception/access "warranting" provisions of the Act.

9. An analysis of this broader legislative context is essential to developing a framework within which meaningful comparisons can be made between:

   a. privacy interests and competing interests; and

   b. alternative means of mitigating privacy risks.

"Compliance" is not the primary objective

10. The Office of the Privacy Commissioner has urged that this PIA "should consider privacy risks beyond legal compliance". On this footing, it is suggested that:

    a. "Assessing legal compliance is necessary but not sufficient"; and

    b. GCSB activity should "aim to comply with the Privacy Principles as much as possible given the context (and without using the [statutory] exceptions to the principles").

11. This advice is instructive to the extent that it suggests an approach that would require GCSB to (i) consider principles it is not statutorily bound to consider but (ii) temper the application of those principles in light of the unique context in which GCSB operates.

12. This PIA follows that approach. This PIA is sought during a "design and build" phase of key elements of the Project. The recommended approach would identify measures that can be reasonably taken to mitigate privacy impacts, whether "required" to be taken or not.

13. Common to a legal compliance approach and the approach urged by the Office of the Privacy Commissioner is the critical and challenging task of determining means of appropriately weighing privacy interests and competing interests. As with any weighing of interests, ultimately this is a matter of judgement. As noted, however, guidance as to the significance of certain privacy principles can be found through close analysis of the legal context in which GCSB operates. A key component of this assessment, therefore, is an analysis of the GCSB Act through a privacy lens.

14. The analysis that follows demonstrates that the GCSB Act was intended to, and does, contain highly effective constraints over GCSB activity, including IACS activity that would be undertaken pursuant to the Project.

Work Undertaken

15. Preparation of the first PIA entailed:

    a. gathering and review of information about the Project;
    b. consultation with GCSB personnel;
    c. preparation of and review of feedback on an initial consultation document: "Broad Brush Scoping of VALENCE Privacy Implications" (VALENCE being a predecessor project);
    d. gathering and review of information concerning PIA best-practice;
    e. meetings with staff of the Office of the Privacy Commissioner;
    f. development of a suitable methodology for approaching privacy issues in the context of IACS services;
    g. meetings with key stakeholders including: IACD staff; IT/Information Security staff; Chief Legal Counsel; Head of Compliance; the Office of the Privacy Commissioner;
    h. preparation of and consultation on a draft report;
    i. review of documentation concerning revised scope of the Project;
    j. submission of draft for Review; and
    k. preparation of the final report.

16. As noted at the outset, preparation of this updated PIA has entailed consideration of changes to the Project activities and a re-assessment of privacy impacts in light of both those changes and steps taken by GCSB to implement recommendations made in the first assessment.

2. METHODOLOGY

17. This PIA entails the following analyses:

a. **Legal analysis** – an analysis of privacy impacts of concern, based upon an analysis of the applicable legal context.

b. **Activity analysis** – a breakdown of Project activities based on technical IAC input.

c. **Impact analysis** – identification of privacy impacts.

d. **Summary and Recommendations**.

3. LEGAL ANALYSIS

18. As noted at the outset, rather than adopting a strict "legal compliance" approach, this PIA adopts the approach recommended by the Office of the Privacy Commissioner – namely, an approach that seeks to maximally apply all of the information privacy principles, albeit "in a manner compatible with the requirements of national security". As also noted, however, both "compatibility" and "the requirements of national security" are elastic concepts. Even on the Commissioner's suggested approach, analysis of the legal context within which GCSB operates is necessary to identify benchmarks that might enable the meaningful weighing of "national security" interests and "privacy" interests.

19. This would include analysis of:

    a. privacy principles that must to some extent be given effect, despite countervailing national security interests; and
    b. aspects of the GCSB Act that are clearly privacy-oriented.

Privacy Principles

Information Privacy Principles under the Privacy Act

20. The IPP concern the collection, use and retention of "personal information". "Personal information" is defined as "information about an identifiable individual" (whether the individual is identified in the information or not). This does not include information about an organisation. Information can be "personal information" whether or not it is sensitive or private. The notion is considered more closely in Part 5.

21. Only one of the IPP confers legally enforceable rights. However, (i) contravention of an IPP constitutes an interference with privacy that may sustain a complaint to the Privacy Commissioner and (ii) as an "agency" as defined by the Privacy Act, GCSB is required to observe certain IPP.

22. Complaints of interference by GCSB stand to be referred to the Inspector-General of Intelligence and Security: s 72B of the Privacy Act.

23. Under the Privacy Act, most of the principles do not apply to intelligence agencies. Section 57 exempts intelligence agencies from adherence to the following principles:

- Principle 1: Collection for necessary and lawful purpose
- Principle 2: Information to come from the individual concerned
- Principle 3: Certain advice to be provided to the individual concerned
- Principle 4: Collection method is to minimise intrusion and be lawful
- Principle 5: Reasonable controls over storage
- Principle 8: Accuracy to be determined before use
- Principle 9: Retention only so long as necessary
- Principle 10: Limits on use for purposes other than purposes of collection
- Principle 11: Limits on disclosure other than for purposes of collection

24. The rationale for certain of these exemptions is not obvious – the exemption from the principle that collection should be for a necessary and lawful purpose being an obvious example.

25. The principles that do apply under the Privacy Act are:

- Principle 6: Entitlement to access information

- Principle 7: Entitlement to correct information
- Principle 12: Restrictions on use of unique identifiers

26. The singling out of Principles 6 and 7 – conferring entitlements to access to and the correction of collected information – is curious. Section 27 of the Privacy Act entitles GCSB to deny access to information where disclosure would be likely to prejudice either (i) the security or defence of New Zealand, (ii) the international relations of the Government of New Zealand or (iii) the entrusting of information to the Government of New Zealand. GCSB's operational security (OPSEC) requirements are such that, in most cases, disclosure is likely to have one of these effects. A denial of access on such grounds will affect compliance with the Principle 7 entitlement to correct information: that entitlement is afforded only by providing access.

IPP under the GCSB Act

27. Under s 25A of the GCSB Act, GCSB must formulate a policy that applies specified information privacy principles. Such a policy is presently under consultation.

28. Section 25A does not refer to the IPP per se but the principles it specifies squarely accord with certain of the IPP. Each of these principles relates to "personal information". "Personal information" is undefined but can sensibly be interpreted by reference to the Privacy Act, namely as "information about an identifiable person".

29. The principles can be summarised as follows:

- Principle 1: Collection reasonably necessary and connected to GCSB function
- Principle 5: Reasonable controls over storage and unauthorised disclosure
- Principle 8: Accuracy to be determined before use
- Principle 9: Retention only so long as necessary

30. The requirement to observe these principles is conditioned by the requirement that they be applied "in a manner compatible with the requirements of national security". This underscores the observation made earlier: undertaking a PIA in this setting is challenging given the pull of national security imperatives. However, as also noted, the principles required to be reflected in a personal information policy at least point to those areas in which privacy interests are expected to be afforded some weight, despite strong competing interests. Indeed, as seen in the section that follows, principles 1, 5 and 9 are supported by provisions within the GCSB Act.

Other privacy-oriented provisions under the GCSB Act

31. Aside from s 25A, potentially privacy-oriented aspects of the Act include:

a. general "principles" governing the exercise of any powers conferred by the GCSB Act;
b. specific criteria governing the issue of "access authorisations" (and "interception warrants");
c. a duty to minimise impacts upon third parties; and
d. controls over the use of acquired information.

The relevant provisions of the Act are considered below.

Governing "principles" of the Act

32. Under s 8D of the GCSB Act, "in performing its functions under this Act" the "GCSB" must (amongst other things) "act in accordance with New Zealand law and all human rights standards recognised by New Zealand law, except to the extent that they are, in relation to national security, modified by an enactment".

33. The IPP constitute privacy "standards" in New Zealand. Their application is modified by the Privacy Act itself, precisely on account of the "national security" context in which GCSB operates. Section 8D adds nothing to this analysis.

Section 14: Collection constraints are limited to "private communications"

34. Section 14 is a key provision of the GCSB Act. Its purpose is to protect the privacy of New Zealand citizens or permanent residents by preventing any activity for the purpose of intercepting the private communications of such persons.

35. Section 14 does not apply to IACS activities. It applies only to GCSB's foreign intelligence gathering activities. However, it would be wrong to assume that communications privacy of affected persons is irrelevant in the context of IACS.

    a. The likely purpose of the restricted application of s 14 is to enable IACS services to be provided at all – not to suggest that IACS activities may proceed irrespective of privacy effects.
    b. To ignore privacy ramifications would run counter to (i) the s 25A requirement for a privacy policy and, more significantly, (ii) the s 15A warrant/authorisation requirement for "satisfactory arrangements" to ensure that the means of collection is reasonable, given the objectives of collection.

36. Nonetheless, it is instructive to note that, even when s 14 applies, it serves to protect only "private communications" – and that "private communication" is defined fairly narrowly.

37. A "private communication" is a communication made in circumstances reasonably indicating that the parties "desire it to be confined to the parties". Further, it cannot be a communication that the communicants ought reasonably expect might be intercepted without their consent.

38. This definition does not appear to recognise privacy interests in metadata (or, as termed by the Office of the Privacy Commissioner, per the Cybercrime Convention, "traffic data") that is generated consequent upon a communication. This is not information that is confined to the parties, let alone intended to be so confined. Nor is it obvious that the communicants could even be considered "parties" to metadata transfers.

39. That the legislature, in the context of foreign intelligence gathering, has used a fairly narrow definition of "private communication" to strike a balance between national security imperatives and privacy concerns is instructive in assessing where that balance should lie in the context of IACS services.

40. Accordingly, this PIA proceeds on the basis that particular care should be taken to minimise the collection of "private communications", as defined in the Act.

Section 15A: Collection-oriented criteria governing the issue of "access authorisations" and interception warrants

41. Section 15A of GCSB Act is a central provision of the Act because it governs the issuing of warrants and authorisations that enable most of GCSB's collection activities. Activities not governed by s 15A are those that *[Text removed under section 6(a) of the Official Information Act 1982]* do not entail the connection of an "interception device" or the installation of a listening device in a particular place. Authority to collect in that setting can be issued by the Director under s 16 of the Act. There are no statutory criteria governing the issue of such authorisations.

42. That said, the Director alone cannot authorise any interception of communications of New Zealand citizens or permanent residents: a s 15A authorisation, issued jointly by the Responsible Minister and the Commissioner of Security Warrants, would be required.

43. Section 15A requires the issuing agency (whether the Minister responsible solely or jointly with the Commissioner for Security Warrants) to be satisfied that, essentially, (i) the interception or access sought is justified by the value of the information sought and (ii) there are "satisfactory arrangements" to ensure that collection activity is undertaken both for the purpose for which authorisation is sought and in a reasonable manner, given the objectives of collection.

44. These "satisfactory arrangements" checks were introduced as part of recent amendments. They strongly suggest a focus upon privacy protections relating to the purpose and manner of collection.

Section 24: Collection methods to minimise third party impacts

45. Section 24 imposes a duty upon GCSB personnel to "take all practicable steps that are reasonable in the circumstances to minimise the likelihood of intercepting communications that are not relevant to the persons whose communications are to be intercepted".

46. This provision is clearly oriented to GCSB's foreign intelligence gathering function rather than its IACS function. Nonetheless, it is further evidence of legislative concern to ensure appropriate control over the manner in which GCSB activities are conducted, notwithstanding the national security imperatives at play.

Section 23: Retention and use of information

47. Inherent in the function of intelligence-gathering is the prospect of acquiring information other than that sought. Section 25 (considered below) allows for the sharing of such "incidentally obtained intelligence" for certain specified purposes. Section 23 requires the destruction of information that neither:

    a. qualifies for retention under s 25;
    b. protects/advances the Bureau's objectives; nor
    c. protects/advances the Bureau's foreign intelligence or IACS related functions.

48. The structure of this provision is instructive in that it suggests a presumption in favour of destruction: all information collected must be destroyed unless it qualifies for retention.

49. Further, the obligation to destroy information that fails to meet any of these criteria is couched in strong terms: "every person... must, as soon as practicable after the interception, destroy...".

50. This PIA therefore proceeds on the basis that appropriate destruction policies and practices are very important.

51. That conclusion is supported by both the following analysis of s 25 and the fact that s 25A of the GCSB Act requires the promulgation of a policy ensuring that there are reasonable controls over storage and that information is retained only so long as necessary.

52. Even though s 23 (and s 25) runs counter to principle 10 of the IPP (limits on use for other purposes), the strong framing of the obligation to destroy clearly indicates that close attention be paid to ensuring that information that is retained for particular purposes be used only for those purposes.

Section 25: Sharing of information

53. As noted, under s 25 certain "incidentally obtained intelligence" may – despite an apparent default position in favour of destruction – be retained and shared.

54. The definition of "incidentally obtained intelligence" is oriented to the foreign intelligence gathering function: it refers to intelligence obtained in the course of obtaining information about the "capabilities, intentions or activities of foreign organisations or foreign persons", namely information that satisfies precisely the definition of "foreign intelligence". That said, the information sought by Project activities (information concerning malicious cyber activity) satisfies this definition too. Section 25 cannot be said to be inapplicable to IACS activities.

55. Section 25 enables "incidentally obtained intelligence" to be retained and shared only for certain purposes, namely the purposes of:

a. preventing/detecting serious crime;
b. preventing/responding to threats to life; and
c. identifying/preventing/responding to threats to national security.

56. The gravity of these purposes supports the conclusions reached above: privacy protections concerning both (i) destruction and (ii) use are very important.

Analysis

57. Controls required to be implemented under the Privacy Act are clearly important controls. They are:

a. Controls enabling access to information
b. Controls enabling the correction of information
c. Controls over the use of unique identifiers

58. Equally, controls that must be the subject of a personal information policy under s 25A of the GCSB Act are important controls. They are:

a. Controls ensuring collection for necessary and lawful purpose
b. Controls over storage and unauthorised disclosure
c. Controls ensuring accuracy is determined before use
d. Controls ensuring retention only so long as necessary

59. Analysis of the GCSB Act more broadly indicates a need for the following controls (refer the underlining in the previous section):

a. Controls to minimise the collection of "private communications", as defined in the Act
b. Controls over the purpose of collection
c. Controls over the manner of collection
d. Controls ensuring that information is destroyed unless required and retained only so long as necessary
e. Controls ensuring that information retained for particular purposes is used for only those purposes
f. Attendant controls over access to retained information

60. There are clear overlaps in these requirements. They are shown in the following table, which relates the requirements to the key phases of information management.

Content and Sources of GCSB's Privacy Related Obligations				
Activity	**Control purpose & attendant principle**	**Section 25A GCSB Act**	**GCSB Act generally**	**Privacy Act**
Collection	**Purpose:** Collection for necessary and lawful purpose (Principle 1)	Collection of personal information to be reasonably necessary for a purpose connected to Bureau function	Collection is for a Bureau function	
	Method: Manner of collection to be reasonable (Principle 4)		"Satisfactory arrangements" to ensure manner of collection is reasonable	
	Scope: Collection of "private communications" to be clearly justified (Principle 4)		Collection of "Private communications" of NZers to be minimised.	
Storage	Collected information is securely held (Principle 5)	Reasonable security safeguards to be taken against loss, unauthorised access, disclosure or modification of personal information	"Satisfactory arrangements" to ensure warranted collect is not used other than as necessary in the performance of Bureau functions	
Use	**Verification:** Information is checked for accuracy before use and data subjects have rights of access and correction (Principles 6,7 and 8)	Reasonable steps to be taken to ensure retained personal information is accurate		Principles 6 & 7: Data subjects to have access to and ability to seek correction of collected information
	Management: Information management should not entail the assignment of unique identifiers unless necessary (Principle 12)			Principle 12: Information management should not entail the assignment of unique identifiers unless necessary
	Application: Collected information is used only for lawful purpose (Principle 10)	Reasonable security safeguards to be taken against "misuse" and unauthorised use of personal information	"Satisfactory arrangements" to ensure warranted collect is not used other than as necessary in the performance of Bureau functions	
	Sharing: Sharing to occur in a controlled manner (Principle 11)	Sharing to be in a manner that reasonably prevents unauthorised use or disclosure		
Destruction	Information to be destroyed unless required for lawful purpose (Principle 9)	Personal information not to be kept for longer than required	Non-Foreign Intelligence can be retained only if justified by Bureau objective, function or s 25 purposes	

61. As can be seen, certain requirements for controls that are set forth in s 25A are "reinforced" in other ways – notably, controls to ensure that:

a. collection is for a lawful purpose;
b. collected information is used in accordance with the purpose of collection;
c. access to collected information is appropriately regulated; and
d. collected information is destroyed when no longer required.

62. Not shown in the above table are controls relating to principles to which GCSB is not required to observe (whether expressly or impliedly), namely:

- Principle 2: Information to come from the individual concerned (the "data subject")
- Principle 3: Certain advice concerning the fact and purpose of collection to be provided to the data subject

63. These require consideration given the approach taken in this PIA – namely the approach suggested by the Office of the Privacy Commissioner, which requires consideration of all the information privacy principles ("in a manner compatible with the requirements of national security"). Consideration to them is therefore given in the analysis that follows.

4. ACTIVITY ANALYSIS

64. This section generally describes the activities associated with each of the relevant Project activities.

65. [Paragraphs 65 to 102 removed under section 6(a) of the Official Information Act 1982]

5. IMPACT ANALYSIS

General Comments

"Personal Information"

103. As noted in Section 3, this PIA is concerned with the collection and management of "personal information" as defined in the Privacy Act – namely, information about an identifiable person.

104. Case law suggests that information that is merely intercepted – but not recorded – is not necessarily "collected", such that the Privacy Principles might not apply.[1] *[Text removed under section 6(a) of the Official Information Act 1982].*

105. Case law also suggests that the notion of information "about" an identifiable person is an extremely broad concept – and certainly capable of extending to a person's work product in the course of employment. Keystroke logging by an employer (for example) has been held to constitute the collection of "personal information" on the basis that it can be "used to determine how much work [an employee] did, or his style or manner of doing it, or his own choices as to how to prioritize it".[2]

106. Further, the notion of "identifiable" is extremely broad. Certainly, there is no requirement that the person be identifiable solely on the basis of the collected information. It will suffice if there is extrinsic information, known to others, that will render the individual identifiable. *[Text removed under section 6(a) of the Official Information Act 1982].* Indeed, information will "probably" be information about an "identifiable person" even if the only person capable of identifying the individual is the data subject himself/herself.[3]

107. Each of the capabilities analysed in the previous section might entail, in one way or another, *[Text removed under section 6(a) of the Official Information Act 1982].*

108. Accordingly, this PIA proceeds on the basis that internal and external users of affected computer systems have privacy interests in information generated or transmitted by them on those systems and that they are the "data subjects" whose privacy stands to be affected by Project activities.

Section 15A as a means of ensuring appropriate privacy controls

109. As noted in Part 3, s 15A directly regulates certain collection activity undertaken by GCSB, whether for IACS-related purposes or foreign intelligence gathering purposes.

110. Section 15A permits the Director to apply for warrants/authorisations in order to intercept communications or access infrastructure that GCSB "cannot otherwise lawfully" intercept/access. As detailed in Part 4, interception/access in the course of Project activities would be undertaken with the consent of affected ANI, so would appear to be activity GCSB

---

[1] *Smits v Santa Fe Gold Ltd* (1999) 5 HRNZ 586

[2] *Order F2005-003* (June 24, 2005, Parkland Regional Library, Review No 3016) – a decision of the Information and Privacy Commissioner of Alberta, Canada

[3] See Privacy Law & Practice, LexisNexis, at PVA2.12

could undertake "otherwise lawfully". However, this is not the way in which IACS activity is presently administered; indeed, one Project activity (Capability 1) is presently undertaken pursuant to an interception warrant. This is on the basis that the consenting agencies are not the "data subjects" from whom GCSB is collecting information and whose privacy stands to be impacted by that collection, such that it is appropriate that such activity to be subject to scrutiny through the warranting process.

111. It is for this reason that access authorisations are also sought to undertake other IACS activity, outside the scope of Project activity and, accordingly, outside the scope of this PIA (namely, the conduct of "investigations" into cyber-attacks). In keeping with this rationale, it is proposed that Project activity (continue to) be warranted/authorised.

112. Any s 15A authorisation required to enable Project activity must be issued by both the Minister Responsible for the GCSB and the Commissioner of Security Warrants (currently a retired judge of the New Zealand Court of Appeal).

113. There are clear, mandatory statutory criteria regulating collection that must be satisfied before authorisations or warrants can be issued. These are highly relevant to this PIA because they are highly geared toward protecting the privacy interests of persons likely to be affected by GCSB interception activity. This is discussed in more detail in the analysis that follows.

114. There is one exception to the requirement for a warrant/authorisation: Capability 5. Information to be used for Capability 5 purposes will have been collected under Capability 1 and, possibly, Capability 3. However, that initial collection will have been warranted collection. In short, therefore, the controls under s 15A will apply to all information collected through Project activity.

The Inspector-General as a means of ensuring compliance with requisite privacy controls

115. Under s 11 of the Inspector-General of Intelligence and Security Act 1996, the Inspector-General of Security and Intelligence must, on an annual basis, review (i) the effectiveness and appropriateness of compliance systems relating to information management and (ii) legal compliance generally. That extends to reviewing the sufficiency of the privacy policy required under s 25A of the GCSB Act (as discussed in Part 3) and its implementation. It also extends to ensuring compliance with controls essential to the granting of warrants or authorisations (on the basis that they are approved by the Responsible Minister and the Commissioner of Security Warrants as "satisfactory arrangements" under s 15A of the Act). The Inspector-General may also raise with the Responsible Minister any concerns with the sufficiency of "arrangements" approved as "satisfactory".

116. The powers vested in the Inspector-General are therefore available to help ensure both (i) the sufficiency of privacy controls required under any warrant/authorisation and (ii) compliance with any requisite privacy controls – whether required under any warrant/authorisation or under the Act itself.

Principle 1: Collection for necessary and lawful purpose

117. Principle 1 requires that personal information not be collected unless collected for a lawful purpose connected with a function of GCSB and collection is necessary for that purpose.

118. As noted by the Office of the Privacy Commissioner in the course of providing feedback concerning aspects of this PIA, the requirement that collection be "necessary" is to be construed as "reasonably necessary".

119. Each Project activity in some way entails the collection of information from consenting ANI who are, essentially, consenting "customers" of GCSB.

120. The "reasonable necessity" for Project activities is set out in detail in a lengthy "business case" prepared by GCSB for the purpose of securing Project funding. Suffice to say, collection associated with the varying activities is justified on the basis of extant needs and technical advice as to how those needs should best be met.

121. In this respect it can be observed that certain Project activities entail precisely the same kind of IAC activity that the affected ANI (indeed, businesses in general) would themselves undertake for IAC purposes. *[Text removed under section 6(a) of the Official Information Act 1982].* However, this PIA need not second-guess the expert opinions underpinning business case assessments of means and ends. That is because this PIA focuses on those controls (outside the business case approval process) that serve to ensure that collection activity is both lawful and reasonably necessary and, as discussed next, these controls are very much directed toward ensuring that these requirements are met.

122. The most obvious control relevant to Principle 1 is s 15A of the GCSB Act.

123. As set out above, certain intelligence collection activities of GCSB must occur pursuant to either an interception warrant or an access authorisation issued under that section. This requirement is intended to ensure rigorous control over collection activity. Indeed, s 15A expressly requires that both the Responsible Minister and the Commissioner of Security Warrants be satisfied that the proposed collection is "justified" in terms of "the outcome sought to be achieved".

124. Obviously, the issuing of a warrant or access authorisation also satisfies the requirement that collection be lawful and reasonably connected to GCSB functions.

125. Further, consenting ANI will enter into a deed with GCSB that records their consent to the service and that (further) regulates the handling, storage and disposal of collected information.

126. These controls are sufficient to ensure that Project activity will conform to the "lawfulness" and "necessity" requirements of Principle 1. On the rationale pursuant to which warrants/authorisations are sought in the first place (considered above), it is warrants/authorisations that would render these activities lawful. The question of whether particular activities are reasonably necessary is a question that has deliberately been left with the Responsible Minister and the Commissioner of Security Warrants in the course of determining whether proposed activities are "justified" in terms of "the outcome sought to be achieved".

Principle 2: Information to come from data subject

127. Principle 2 requires that any collected personal information be collected "directly from the individual concerned". It advances the interests of data subjects by supporting accuracy in the recording of collected information. (It also serves to notify data subjects of the fact that information is being collected. However, that particular outcome is the focus of Principle 3, which is considered next.)

128. *[Text removed under section 6(a) of the Official Information Act 1982].*

Principle 3: Certain advice to be provided to data subjects

129. Principle 3 requires that data subjects be informed of the fact of collection, the purpose of collection, the intended recipients of collected information and of certain other matters, including the "rights of access" of data subjects to information under other principles.

130. This requirement advances privacy by enabling data subjects to assess the availability and content of personal information about them. However, it is not proposed that any of the intended IACS activities will entail the provision of such advice to data subjects. Accordingly, to the extent that data subjects are oblivious to the fact of collection by GCSB, Project activities would have unavoidable privacy impacts.

131. The significance of this impact might be significantly mitigated by context – in particular by limits upon the privacy expectations of internal and external users of affected systems.

132. For example, data subjects might be informed that the affected organisation will collect information for IACS purposes – even if they are not told that GCSB will be the collecting agency. This is probable where the affected computer system is a corporate system used solely to support internal corporate services. In that setting, data subjects who are employees (or other internal users) can be expected to accept, as an express condition of accessing the affected computer system, that communications generated on or transmitted via that system could be retained and accessed by IT security personnel for IACS related purposes. The imposition of such internal access requirements could – and should – be imposed as conditions of Project activity. Under the terms of deeds currently used to record the consent of affected ANI, ANI are indeed required to apprise "persons whose communications will be accessed and/or retained" that such access/retention will occur.

133. Such express access conditions would not mitigate the privacy impacts upon external third parties communicating with internal users via affected systems. *[Text removed under section 6(a) of the Official Information Act 1982].* Any third party communicating with a business entity (including a Government entity) would reasonably expect that entity to at least scan incoming communications. Such persons would also reasonably expect such communications to be accessible by persons granted system administrator access for IACS related purposes.

134. That said, the foregoing analysis is less viable in the context of outward facing organisations, *[Text removed under section 6(a) of the Official Information Act 1982].*

135. Even in that context, however, privacy impacts are limited by the limited effect played by Principle 3 – in the context of Project activities – in supporting downstream interests to access and seek the correction of collected information (also protected by the Privacy Principles). The impact upon these interests is limited because Project activities do not closely engage those other downstream interests. (This point is explained below, in the discussion of Principles 6 and 7.) In this respect, the impact of non-compliance with Principle 3 is reduced.

136. To the extent that compliance with Principle 3 also triggers entitlements to refuse to supply information or to contest the fact of collection, again the essential character of Project activities as IACS activities is highly relevant. As noted, IACS activity, such as *[Text removed under section 6(a) of the Official Information Act 1982]* is a prudent, ubiquitous business practice. Accordingly, requirements to accept such practices are commonplace pre-requisites to system access by internal users. The impact of non-compliance with Principle 3 in terms of undermining "rights" to refuse to "provide" information is commensurately, and markedly, reduced. Although external users might not surrender such rights in that way, the ubiquity of IACS related data interception and retention is such that external users can reasonably be presumed to have waived them by simply electing to communicate via the ANI's computer system.

137. To the extent that compliance with Principle 3 triggers entitlements to contest not the collection of but the handling of collected information, it is highly relevant that (i), with the possible exception of Capability 5, all collection activity must be either warranted or authorised by the Responsible Minister and the Commissioner of Security Warrants, (ii) warrants or

authorisations cannot be issued unless there are "satisfactory arrangements" regulating the scope of collection activity and the handling of collected data and (iii) means of auditing compliance with these arrangements is a prime concern of the Inspector-General of Intelligence and Security. This framework is more fully considered in relation to Principle 4 (next) and elsewhere in this PIA. In short, this framework is intended to be highly protective of the privacy interests of data subjects. To the extent that Principle 3 is auxiliary of these interests, this significantly mitigates the impacts of any non-compliance with that principle.

138. This observation is particularly relevant given that it is not known with precision the precise contexts in which certain activities will be undertaken. *[Text removed under section 6(a) of the Official Information Act 1982]*. Any such discrimination would significantly reduce the privacy impacts of non-compliance with Principle 3. However, even were such discrimination not possible, the downstream impacts of non-compliance with Principle 3 must still be justified in terms of s 15A and, on that account, regarded as acceptable in light of "satisfactory arrangements" regulating the collection and handling of information.

139. From a pure compliance perspective, Principle 3 is another principle with which GCSB is neither explicitly nor implicitly required to comply. That point aside, however, non-compliance with Principle 3 can be justified by reference to exemptions contained in paragraph 4 of Principle 3 itself, as follows.

    a. Pursuant to paragraphs 4(c) and (d) These paragraphs comprise exemptions where compliance would prejudice either the detection of offences or the purposes of collection. These paragraphs would apply because non-compliance would be for the purpose of maintaining operational security over GCSB activity, which (in turn) (i) enhances the information security of the affected organisation by ensuring it is not highlighted to adversaries as an entity requiring to be attacked in a more sophisticated manner and (ii) guards against the prospect that adversaries will not shift their attentions to "softer" targets.
    b. Pursuant to paragraph 4(f) This paragraph exempts compliance where the agency reasonably believes the information will not be used "in a form in which the individual concerned is identified". This exemption would apply to Capability 1 "Level 1" activity and to any other activity similarly undertaken as an initial stage of a staged approach. That is because, although those IACS activities entail the collection of information about "identifiable" persons, they do not entail the human analysis of information that actually identifies those persons. In that sense, only information identifying particular terminals is "used".

140. In summary, not only would the privacy impacts of non-compliance with Principle 3 be significantly reduced given the context in which Project activities would occur, non-compliance is readily justifiable by reference to exemptions to Principle 3. In any event, no "compliance" issues arise for the reason that Principle 3 is not a principle with which GCSB must comply.

Principle 4: Collection method to minimise intrusion and be lawful

141. Principle 4 requires that personal information not be collected by unlawful means or by any means that, in the circumstances, is "unfair" or "intrude[s] to an unreasonable extent upon the personal affairs of the individual concerned".

142. *[Text removed under section 6(a) of the Official Information Act 1982].*

143. Clearly, each capability reflects varying levels of "intrusion". The sufficiency of the justifications for these intrusions are concerns of Principle 1. As noted in the discussion of Principle 1, a detailed business case has been prepared justifying the above collection activity on the basis of

expert assessments of (i) extant needs and (ii) technical solutions that best meet those needs. This principle, Principle 4, is concerned with the latter: the manner in which information is collected.

144. As noted already, certain Project activities are commonplace kinds of IACS activity, being activities commonly undertaken by individuals and businesses requiring access to the internet. In the discussion of Principle 1, Capability 1 was cited as an obvious example. Indeed, all Project activities entail the deployment of readily available commercial tools, the use of which by organisations significant enough to constitute ANI would be unremarkable (and might be expected).

145. Beyond those observations, the warranting/authorisation process is the primary means of ensuring that collection activity is reasonably necessary. This process is particularly important even though Project activity entails merely the deployment of commercially available tools. For example, as noted in the discussion of Capability 2 in Part 4, commercial tools available to support Capability 2 offer varying "feature sets" that, in turn, enable different kinds of (intrusive) activity. The warranting/authorisation process will be the mechanism through which proposed feature sets are ultimately approved as, essentially, reasonable ("satisfactory").

146. Being the provision that regulates this process, s 15A of the GCSB Act is the critical provision.

147. A key driver of the amendments leading to the enactment of s 15A was the need to ensure the continued lawfulness of GCSB's information assurance any cyber security activities. Those amendments also rendered the processes for obtaining interception warrants and access authorisations far more prescriptive than previously. As shown by the analysis in Part 3, the "reasonable necessity" requirements of Principle 4 are shared by s 15A: information assurance related warrants and authorisations cannot be issued unless both the Minister Responsible for the GCSB and the Commissioner for Security Warrants are satisfied that GCSB is capable of implementing "satisfactory arrangements" appropriately regulating what information is collected, how it is collected and how it is stored and used. Of particular relevance to Principle 4 is s 15A(2)(c), which requires that the Minister and Commissioner be satisfied that "the outcome is not likely to be achieved by other means".

148. Further, it is the responsibility of the Inspector-General of Intelligence and Security to audit the sufficiency and implementation of controls in these, and other, respects.

149. This framework is intended to ensure not only that information assurance and cyber security activities are undertaken only pursuant to an appropriate legal authority (Principle 1) but that the manner in which it is undertaken is subject to externally audited controls ensuring that such activities are appropriate, including proportionate in terms of balancing privacy and security interests (Principle 4). Further, this framework will be supported by internal audit controls implemented by GCSB's compliance team.

150. These controls are designed to be, and are here considered to be, sufficient to ensure that Project activities will conform to the requirements of Principle 4. The highly restrictive approach taken to the warranting of Capability 1 activity evidences this. As noted, (i) Capability 1 activity currently proceeds only pursuant to, essentially, a staged approach that, in the first instance, restricts the access of analysts to "personal communications" and (ii) access to personal communications is granted only pursuant to a further interception warrant on the basis of demonstrated need. *[Text removed under section 6(a) of the Official Information Act 1982].* Their implementation clearly demonstrates the "privacy reach" of the GCSB Act, in particular in relation to Principle 4.

Principle 5: Reasonable controls over storage

151. *[Text removed under section 6(a) of the Official Information Act 1982]*

152. The Project's principal means of accessing collected information is via a purpose-built analytical environment. This environment is described as an "analytical realm". *[Text removed under section 6(a) of the Official Information Act 1982]*

153. *[Text removed under section 6(a) of the Official Information Act 1982]*

154. Access through the analytical realm is regulated by system engineers who:

    a. ensure that the systems operate in a manner that meets security standards, as directed by the GCSB CIO;
    b. develop, implement and maintain accesses as required; and
    c. undertake auditing for the purpose of ensuring compliance with security and access standards.

155. It is proposed that all access to storage enclaves be logged. Logs would be subject to internal audit by the GCSB compliance team and to external audit by the Inspector-General.

156. In order to raise the requisite warrants or authorisations, these controls would have to be accepted as sufficient by the Minister Responsible and the Commissioner of Security Warrants. There is no reason to suspect they would not be considered sufficient. They have already been accepted as sufficient to support the issue of existing Capability 1 interception warrants.

157. Access permissions required to be administered pursuant to the above controls would be set in accordance with the terms of the overriding interception warrants or access authorisations.

158. Accordingly, the warrant/authorisation framework considered above would ensure suitable safeguards over not only how information is collected but how it is stored and accessed – in particular by ensuring that permissions are granted only as required for the purposes for which collection occurs.

159. Relevant too is the reduced potential for violation of storage and access controls. This arises through GCSB's extraordinary INFOSEC controls. These include not only technological controls *[Text removed under section 6(a) of the Official Information Act 1982]* but also physical controls (regulating the movement of information, media devices and people into and out of premises). They also include standard operating procedures, including routine requirements concerning the classification of information and protocols governing extraordinarily controlled information (ECI). Security vetting and cultural norms within the intelligence community are strong underpinning controls.

160. These more general INFOSEC controls also constitute effective means of meeting the Principle 5 requirement that personal information be shared only pursuant to reasonable measures to prevent unauthorised disclosure – particularly handling restrictions attendant upon the routine classification of information. So too are those Capability 1 controls that must be implemented before Capability 1 collect may be shared. As noted, these preclude the sharing of any "personal communications" other than in support of the functions of certain agencies for IACS purposes.

161. In summary, the warranting/authorisation process is intended to ensure that collected information is sufficiently protected against loss and misuse, within the meaning of Principle 5. Further, compliance is underpinned by stringent INFOSEC controls that more generally apply. Certain of these address the additional Principle 5 requirement for reasonable measures

preventing misuse by any third party recipients – particularly handling restrictions attendant upon the routine classification of information.

Principles 6 & 7 – Data subjects to be provided access and rights to request correction

162. Certain of the Privacy Principles concern the interests of data subjects in ensuring that collected information is accurate. These include the principles requiring that collected information be (i) collected from the data source (Principle 1), (ii) checked for accuracy etc before use (Principle 8), (iii) accessible to the data subject (Principle 6) and (iv) amenable to correction at the request of the data subject (Principle 7).

163. As noted above, for reasons of (principally) national security it is not proposed that data subjects (ie users of affected computer systems) be informed, under Principle 3, of the fact of data collection by GCSB and of their rights to seek correction to that information. Rather, consent to access/interception activity will be granted at the organisation-level.

164. This has obvious ramifications for the ability of data subjects to gain access to collected information (Principle 6) and to request the correction of that information (Principle 7): data subjects are unlikely to exercise rights concerning access to collected information if oblivious to that collection.

165. That said, data subjects might nonetheless make requests under Principle 6 for the simple purpose of learning whether or not GCSB holds personal information concerning them. Accordingly, GCSB's general processes for dealing with such requests are relevant.

166. Under the Privacy Act, Principle 6 is subject to section 27 of that Act. Section 27 permits an agency to "refuse to disclose any information requested pursuant to Principle 6" if disclosure would be likely to prejudice the security or defence of New Zealand.

167. As noted, the prospect of such prejudice is one of the bases upon which data subjects are not apprised of the fact of collection by GCSB in the first place. Of course, that prospect arises equally in the context of advising data subjects upon request.

168. That said, GCSB currently adheres to a practice (to be enshrined in a policy) of acceding to Principle 6 requests where the requestor is a "person of unconventional perceptions" – a broad class of persons whose mental condition might be adversely affected by a "neither confirm nor deny" response. That practice has been reached following consultation with the Office of the Privacy Commissioner.

169. In other situations, the impact of refusals to grant access under Principle 6 (and, therefore, of any non-compliance with Principle 7) are significantly mitigated by negligible risk that collected information might be "inaccurate". Not only is personal information collected from the data source (per Principle 2, considered above) it is not altered through any recording process. Rather, as noted in the discussion concerning Principle 8 (below), "collected" information is subjected to a screening process. Although, as discussed in Part 3, certain Project activities entail the duplication of information prior to screening (and the retention of that information for the purpose of future screening), it is the essence of duplication that information is recorded exactly as transmitted or generated.

170. The effects of non-compliance are therefore limited to data subjects simply not knowing whether GCSB holds their personal information. This impact too is reduced where data subjects at least understand that information might be collected for IACS purposes. As noted earlier (in the context of Principle 3), it is recommended that assisted ANI be required to provide such advice to internal users of their systems.

171. Obviously, the requirements of Principle 7 can be met only where a Principle 6 request has been met: a data subject cannot seek correction of information to which he/she is not granted access. Accordingly, the need to comply with Principle 7 stands to be read in light of the exemptions to Principle 6.

172. Principles 6 and 7 are not principles required to be given effect under the GCSB Act. (As noted in Part 3, controls under the GCSB Act ensuring the accuracy of collected information are limited to those required by Principle 8: namely, controls establishing reasonable steps to ensure accuracy before use – considered below). However, even were it otherwise exemptions to Principle 6 would apply, on the basis of "likely to prejudice the security or defence of New Zealand".

173. In summary, even though information is neither collected nor used on the basis of the "accuracy" of its content, (i) it is, nonetheless, "accurately" recorded by way of digital duplication and (ii) data subjects are likely to reasonably expect (if not know) their communications are being collected for IACS-related purposes. Accordingly, the effects of non-compliance with Principles 6 and 7 are significantly reduced. Further, such non-compliance is permissible under exemptions to Principle 6 (which logically extend to Principle 7).

Principle 8: Accuracy to be determined before use

174. Principle 8 requires that "where an agency collects information directly from the individual concerned", the agency shall not "use" that information without taking "such steps (if any) as are, in the circumstances, reasonable" to ensure that "having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, compete, relevant, and not misleading". As noted in Part 3, although GCSB is exempted from compliance with this Principle under the Privacy Act, it is mirrored in identical terms under s 25B of the GCSB Act.

175. Rather than prescribing particular steps, Principle 8 is self-calibrating: essentially, it requires such verification steps as are "reasonable", given the purpose of collection. Context, therefore, is critical. As Principle 8 itself expressly countenances, the context might suggest that no steps are required.

176. The context of Project activities is the collection and use of information in a manner that is entirely independent of the "accuracy" of the content of any collected personal information. Information is collected only because it is "data" generated on or transmitted via a particular information infrastructure. That is because the purpose of collection is to detect any data that might constitute a vector of cyber-attack. Although some activities entail the interception of only particular types of data, such data is collected indiscriminately – and the relevant characteristics of those types of data have nothing to do with the accuracy of the "content" of any "personal information" it might contain. The interests protected by Principle 8 are commensurately (ie, markedly) diminished.

177. In context, reasonable "verification" steps would be limited to ensuring accuracy in any duplication processes *[Text removed under section 6(a) of the Official Information Act 1982]*

178. Although it is beyond the scope of this PIA to technically audit Project capabilities in terms of their ability to deliver their intended outcomes, it is notable that, where duplication comprises an element of Project activity, accuracy is obviously critical to the intended IACS delivery.

179. In summary, Principle 8 requires only the taking of such steps as are reasonable in the circumstances and, in the context of Project activities, such steps (if any) extend merely to ensuring the delivery of a capability that is required in any event – namely, an "accurate"

duplication capability. There is no reason to presume that such a capability will not be provided. Rather, there is every reason to presume it will be.

Principle 9: Retention only so long as necessary

180. Principle 9 requires that personal information not be kept for longer than is required for the purposes for which it may lawfully be used. As with Principle 8, although GCSB is exempted from compliance under the Privacy Act, this principle is mirrored in identical terms under s 25B of the GCSB Act.

181. Obviously, this principle presumes that information is "kept" – not simply screened. Nonetheless, Principle 9 is relevant to all Project activities to the extent that, as discussed in Part 3, even screening activities can result in the retention of personal information generated as a result of screening activity.

182. GCSB has not formulated retention and destruction policies for all Project activities. However, where information is collected pursuant to a warrant or access authorisation, such policies (and supporting controls) must satisfy the Responsible Minister and the Commissioner of Security Warrants as being supportive of a broader objective of ensuring that collected information is not used in a manner "beyond what is necessary for the proper performance of a function of the Bureau".

183. The warranting/authorisation process has been shown to effectively regulate GCSB practices in this respect. Existing interception warrants that support existing Capability 1 activity, for example, were issued on the basis that collected information be electronically date-stamped at the time of collection and be automatically destroyed *[Text removed under section 6(a) of the Official Information Act 1982]*. Retention for that period was accepted as justifiable on the basis that it supports retrospective screening for advanced threats that might not have been identified at the time the information was collected.

Principle 10: Limits on use for purposes other than purposes of collection

184. Principle 10 prohibits the use of information other than "in connection with" the purpose(s) for which it was obtained. It is subject to exemptions.

185. The manner in which information obtained through Project activities is stored does not render it readily amenable to use for any purpose other than the provision of IACS services (or, for that matter, for any other purposes). That is because the purpose of collection is the detection of malicious cyber activity and, as noted in the discussion of Principles 6 and 7, meeting this purpose does not require *[Text removed under section 6(a) of the Official Information Act 1982]*.

186. That said, it is technically possible for access tools and privileges to be abused for the purpose of deliberately accessing the "content" of collected information. Accordingly, compliance with Principle 10 is, in the first instance, a function of the effectiveness of controls regulating access to collected information.

187. Access controls – including controls against "misuse" – are discussed in relation to Principle 5, above. In short, access to collected information will occur through the analytical realm – access to which, in turn, is regulated by system engineers who:

a. ensure that the systems operate in a manner that meets security standards, as directed by the GCSB CIO;
b. develop, implement and maintain accesses as required; and

c. undertake auditing for the purpose of ensuring compliance with security and access standards.

188. Compliance with (downstream) Principle 10 requirements that accessed information be used only for proper purposes stands to be enforced through the same controls that support compliance with (upstream) access restrictions (described in relation to Principle 5), namely robust technological and physical INFOSEC controls supported by security vetting and cultural norms within the intelligence community. Highly relevant too is the ability of the analytical realm to log all access and activity and to make those logs available to support internal and external audit (including through the office of the Inspector-General of Intelligence and Security).

189. Further, it is relevant that Project activities will be undertaken only pursuant to a warrant or authorisation on the basis of controls that constitute, to the satisfaction of the Responsible Minister and the Commissioner of Security Warrants, "satisfactory arrangements" with respect to the handling of collected information generally. Indeed, s 15A(2) (which governs the issuing of warrants and authorisations) expressly requires controls over use: namely "satisfactory arrangements... to ensure that nothing will be done in reliance on the warrant or authorisation beyond what is necessary for the proper performance of a function of the Bureau".

190. The extent of this control – being tied to the performance of a "function of the Bureau" – requires consideration because the functions of the Bureau include the gathering of foreign intelligence as well as the provision of IACS services. In that respect, warrants currently issued in support of Capability 1 and Capability 4 activity have been issued on the basis of controls preventing use for foreign intelligence purposes. That reflects the requirements of section 14 of the Act: under section 14, collection for foreign intelligence purposes cannot extend to the interception of private communications of New Zealand citizens or permanent residents.

191. In summary, controls over access and use that are implementable through the analytical realm (particularly the auditable logging of all access to, and use of, the analytical realm) significantly mitigate the potential for collected information to be used other than for IACS purposes. Further, the warranting/authorisation process constitutes a sufficient framework to ensure that collected information is sufficiently protected against misuse. Further, compliance is underpinned by stringent INFOSEC controls that more generally apply.

192. For completeness, it is noted that Principle 10 is subject to exemptions. Those most likely relevant relate to:

a. avoiding "prejudice to the maintenance of the law" (including the detection and prevention of offences);
b. the prevention or mitigation of "serious threats" to public safety or individual life or health; and
c. use of the information in a form in which the data subject is not identified or for statistical or research purposes that could not reasonably be expected to identify the individual concerned.

193. Practically, there is limited scope for these exemptions to come into play. That is because, as noted above, collected information is organised in such a way that there is limited scope that information relevant to any non-IACS purpose will even be identified.

Principle 11: Limits on disclosure other than for purposes of collection

194. Principle 11 places limits on disclosure of collected information for purposes other than the purposes for which the information was collected.

195. These limits on disclosure parallel the limits on use that are set by Principle 10. They are subject to parallel exemptions.

196. The above analysis concerning the likelihood of "misuse" under Principle 10 is directly relevant in assessing the prospects that collected information will be improperly disclosed (in the sense of being disclosed for non-IACS related purposes). In short, given the unlikelihood that, within collected information, GCSB analysts will identify information warranting disclosure on non-IACS related grounds (whether on grounds justifying disclosure under the exemptions or otherwise), it is unlikely that collected information would be disclosed other than for IACS purposes. As with non-compliance with Principle 10, the risk of non-compliance with Principle 11 is commensurate with the risk of deliberate misuse of those tools for the purpose of exploiting collected information for improper purposes.

197. Accordingly, the access controls analysed in the discussion of Principles 5 and 10 are relevant also in the context of Principle 11. In short, any controls that regulate access to, and use of, collected information will limit the risk that collected information will be exploited for non-IACS related purposes and, on that account, will limit the prospects that it will be improperly disclosed for non-IACS purposes. As discussed in relation to Principles 5 and 10, those controls include not only particular logging and audit controls but more generally applicable INFOSEC controls. Further, in the context of Project activities, those controls must be (i) approved as "satisfactory arrangements" under a warrant or authorisation and (ii) acceptable to affected ANI.

198. There remains the potential that disclosed information will be properly disclosed in the sense of being disclosed for IACS-related purposes but improperly disclosed in the sense of being disclosed to persons not authorised to receive it. That is not an acute risk:

a. an enduring purpose of GCSB IACS-related collection activity is to support IACS efforts more broadly through intelligence-sharing;
b. under s 8A of the GCSB Act, GCSB may share information gathered as a result of IACS activities with any entity authorised by the Responsible Minister to receive it; and
c. the Responsible Minister has authorised sharing with those entities that might have a legitimate interest in IACS-related intelligence.

199. The residual risk of disclosure for IACS-related purposes to "unauthorised" recipients stands to be managed by general INFOSEC controls, including cultural norms within GCSB. In that regard, it is relevant that GCSB's governing legislation has long-placed limits on unauthorised disclosure. This includes not only s 11 (establishing an offence of "unauthorised disclosure of information") but also s 25 in both its current and previous forms.

Principle 12: No unnecessary use of unique identifiers

200. Project activities do not entail the use of unique identifiers.

6. SUMMARY AND RECOMMENDATIONS

Impacts in terms of ensuring "accuracy before use"

201. As noted in Part 3, s 25A requires the adoption of a policy establishing controls ensuring that reasonable steps are taken to ensure that collected information is accurate before use. This is supported by Privacy Act principles (that apply to GCSB) that entitle data subjects to access and seek the correction of collected information

202. Potential "accuracy" impacts are addressed in that (i) Project activities will entail the collection of information that is generated by the data subjects themselves and (ii), to the extent it is recorded, it is digitally duplicated.

No recommendations are made in this respect.

Impacts in terms of providing advice and access to data subjects

203. Most likely, the "accuracy before use" requirement has been imported into the GCSB Act on account of its potential value in the context of GCSB's foreign intelligence gathering function. As discussed in Part 5, in the context of IACS it is inapt.

204. This has flow-on effects in terms of assessing the impacts of non-conformity with other Privacy Principles that are intended to support "accuracy before use" – including those conferring entitlements to access information (Principle 6) and to seek the "correction" of information (Principle 7). In short, the impacts of non-compliance with these Principles are markedly reduced.

205. Nonetheless, the first PIA recommended that, as a condition of receiving GCSB IACS services, ANI be required to notify internal users and (via return emails) external users of their systems that communications via these systems will be accessed for IACS purposes. GCSB has since acted upon that recommendation by incorporating such a requirement as a standard term of its written agreements with ANI. That term reads as follows:

> *The Assisted Entity will advise persons whose communications will be accessed and/or retained through the provision of the Assistance that their communications will be accessed and/or retained for information assurance purposes. Such advice: (a) shall not identify GCSB as an entity undertaking access for such purposes; (b) will otherwise meet GCSB requirements.*

206. GCSB has also advised that "in practice, this [requirement] is anticipated to be met through a variety of means including the ANI's internal IT use policies and practices, their Privacy Statement, or other documents relating to internal and external communications on ANI infrastructure".

207. Compliance by ANI with this term will ensure that data subjects are aware that their communications are being collected for IACS purposes, albeit unaware that it is *GCSB* that is collecting it.

208. Although notification that information will be collected for "information assurance purposes" is sufficiently broad to cover collection for Capability 5 purposes *[Text removed under section 6(a) of the Official Information Act 1982]*. That said:

a. It is unlikely that more explicit advice could be provided to system users without disclosing the potential involvement of GCSB or otherwise compromising essential OPSEC;
b. Consistent with the analysis in Section 4, agreements with ANI will authorise collection for Capability 5 purposes; and
c. System users are at least apprised of the fact of collection.

209. The impacts of incomplete disclosure are relevant to Principle 3, which requires that data subjects be told certain things when personal information is collected. As noted in Section 5 of this PIA, to the extent that data subjects are oblivious to the fact of collection by GCSB (or of use for Capability 5 purposes), Project activities would have unavoidable privacy impacts in terms of denial of access and rights to seek correction.

210. This does not raise compliance concerns. Principle 3 is not a principle with which GCSB is required to comply, whether explicitly or implicitly. That point aside, non-compliance with Principle 6 (denial of access) is justifiable on national security grounds. National security grounds are precisely the grounds upon which data subjects would not be given access to information collected through Project activities.

211. Accordingly, the impacts of non-compliance with Principle 6 (access) and of "non-conformity" with Principle 3 (advice) are not only heavily mitigated by context but are justifiable.

212. The Office of Privacy Commissioner has already recommended that GCSB relax its stance in terms of granting access (and providing advice concerning the fact of collection) where data subjects request advice and access and are "persons of unconventional perceptions". That recommendation has been adopted.

Recommendations:

The standard term contained in written agreements with ANI is broad enough to oblige ANI to notify not only internal but also external users of their systems that communications will be collected for IACS purposes. However, it does not expressly identify external users and could be construed as limited to only internal users. Further, the means through which GCSB expects this requirement to be met are not means that necessarily entail notification to external users. Although GCSB personnel have advised that this standard term is nonetheless construed by ANI as obliging ANI to take these measures, it is recommended that it expressly require ANI to notify external users that communications via affected systems will be accessed for IACS purposes.

Impacts in terms of ensuring collection is lawful and reasonable

213. As noted in part 3, certain privacy controls are particularly significant in the context of GCSB activity in that they are required not only under s 25A but also under either other provisions of the GCSB Act or under the Privacy Act. These include controls ensuring that collection is for a lawful purpose and is reasonably undertaken.

214. In terms of "reasonableness", the sorts of activities proposed to be undertaken are types of detection and disruption activity often undertaken in purely commercial settings for IACS purposes. There is nothing peculiarly intrusive about their delivery in the context of Project activity. The tools to be deployed in relation to each activity are commercially available tools. The point of difference lies in the nature of the threats that GCSB is capable of detecting and disrupting – namely, *[Text removed under section 6(a) of the Official Information Act 1982].*

215. Quite apart from that, all collection for Project activity will be warranted or authorised under s 15A of the GCSB Act. This is clearly significant in terms of ensuring both legality and reasonableness. Warrants/Authorisations will ensure legality. They will not be issued unless

the proposed activity and the attendant privacy impacts are reasonable, in the sense of proportionate to the national security interests at play.

216. The warranting/authorisation framework was amended to achieve precisely this outcome. No further recommendations are made in these respects.

217. The first draft of this PIA (i) regarded Capability 5 as extending to the provision to *[Text removed under section 6(a) of the Official Information Act 1982]* and (ii) indicated that such receipt might not be collection regulated by the warranting process (on the basis that it might not qualify as "interception" by GCSB *[Text removed under section 6(a) of the Official Information Act 1982]*Accordingly, the first draft of this PIA recommended that alternative protections be put in place. In particular, it was recommended that:

a. A mechanism be developed to ensure that privacy intrusions attendant upon Capability 5 activity are proportionate to the national security interests at play; and
b. Such a mechanism ought to entail high-level (likely Director-level) approval on the basis of precisely those factors requiring to be addressed under s 15A. In particular, it should ensure that information to be passed from MSPs to GCSB is not more than necessary to support GCSB's IACS function.

218. However, as now revised Capability 5 will not be extending (at least at this stage) to any collection – rather, it will entail only the use of information collected pursuant to other capabilities, which will be warranted collection. On that basis the earlier recommendations are inapposite.

No recommendations are made in this respect

Impacts in terms of ensuring information is properly used and destroyed when not required

219. Other privacy controls required under s 25A that are "reinforced" under the GCSB Act or the Privacy Act are controls ensuring that:

a. access to collected information is appropriately regulated;
b. collected information is used in accordance with the purpose of collection; and
c. collected information is destroyed when no longer required.

220. As discussed in Part 5, the impacts of Project activity in these respects are principally functions of:

a. access controls;
b. auditability of access; and
c. destruction policies and methods.

221. Access controls are robust. Information will be held in a classified environment accessible to only authorised, cleared personnel. These are supported by extraordinary INFOSEC controls that attend all GCSB activities. All access to information will be logged for audit purposes. Audits will be undertaken both internally through GCSB's compliance team and stand to be externally audited through the office of the Inspector-General of Intelligence and Security. Information will be retained for a reasonable period for purposes for which it was collected. Thereafter, it will be destroyed automatically on the basis of electronic date-stamping at the time of collection – unless exempted from destruction on the basis that retention is needed to support on-going GCSB activities.

222. These controls are sound and, as noted, have already been shown to effectively regulate some Project activities. They will apply to information collected pursuant to all Project activity.

223. GCSB's extraordinary OPSEC measures, supported by the warranting/authorisation framework, will serve to ensure that avenues for potential misuse of collected information (whether through unauthorised access or improper use by authorised personnel) are reasonable.

224. Since the first PIA, GCSB has highlighted that (i) the written agreements with ANI will permit only "Authorised Persons" to access collected information and (ii) Authorised Persons are identified in writing by the Director or a Deputy Director of GCSB. This was known at the time of the first PIA and was one of the reasons supporting the conclusion that controls in this respect are sound.

225. That said, GCSB has made changes to the standard terms of those written agreements that will further improve these controls. The relevant changes are changes to the terms restricting GCSB's ability to share collected information with third parties. These restrictions will apply to "protected information". "Protected information" is defined as *[Text removed under section 6(a) of the Official Information Act 1982]*. "Protected information" may be shared by GCSB with a third party (other than the Responsible Minister and the Minister for National Security and Intelligence) only pursuant to a written agreement between the ANI and the third party (unless the "user" is a malicious actor).

226. GCSB has further advised that the terms of warrants and authorisations currently regulating certain Project activities further restrict sharing: "protected information" may be shared only either:

a) *[Text removed under section 6(a) of the Official Information Act 1982]*

b) *[Text removed under section 6(a) of the Official Information Act 1982]*

227. An examination of current Capability 1 warrants bears out the existence of these additional restrictions. Although, under those warrants, data that is considered to be associated with malicious activity may be retained *[Text removed under section 6(a) of the Official Information Act 1982]*, that is entirely consistent with the purpose for which data is collected in the first place.

228. The first PIA noted also that GCSB has not developed any Project-specific retention and destruction policies. It considered that (i) the *[Text removed under section 6(a) of the Official Information Act 1982]* retention period prescribed under existing Capability 1 warrants is not necessarily appropriate to other Project activity and (ii) the rationale for settling upon that period (ie, the benefit of being able to "retrospectively" scan collected information for different indicia of malicious activity) does not universally apply.

229. GCSB has since advised that warrants and authorisations for all Project activity and all agreements with ANI would require GCSB to retain information for not more than *[Text removed under section 6(a) of the Official Information Act 1982]*. A Cabinet Paper seeking policy approval for Project CORTEX states that information acquired through project activities will be retained for a period of *[Text removed under section 6(a) of the Official Information Act 1982]*.

230. The standard terms contained the written agreements with ANI express the retention and destruction requirements differently but to the same effect, save in one respect. The agreements permit the extended retention of not only data associated with malicious activity but of data that is shared with another entity (in accordance with sharing provisions of those agreements).

231. As noted, compliance will be supported by advanced technical solutions thatwill enable automated destruction of data that reaches its retention deadline.

232. In the absence of a clearly articulated retention and destruction policy, it is not demonstrable that *[Text removed under section 6(a) of the Official Information Act 1982]* is an appropriate period for all information gathered pursuant to Project activities. The first PIA recommended that GCSB develop a retention and destruction policy for each Project activity, taking into account the differing benefits of retention in each case. GCSB has advised that the *[Text removed under section 6(a) of the Official Information Act 1982]* retention period is an interim response to that recommendation and that "specific retention and destruction policies for each Project activity are being developed as the technical details of each activity are finalised". Any such policies should not only stipulate standard retention periods particular to each Project activity they should also regulate the retention of data qualifying for extended retention. It is unlikely that data qualifying for extended retention will, on that account, qualify for indefinite retention, even though "indefinite" retention of such data is permitted under existing warrants.

Recommendations:

a) It is recommended that GCSB develop a retention and destruction policy for each Project activity, taking into account (i) the differing benefits of retention in each case and (ii) the potential need for even data qualifying for extended retention to be destroyed at some stage.

b) To minimise the potential for a breach of sharing restrictions, GCSB should seek consistency in how these restrictions are expressed in warrants/authorisations and in written agreements with ANI.